Azure Network Security – Private Endpoint Hardening with Azure Firewall & Zero Trust Controls

Role: Cloud Security Engineer – Lab Project

Tools: Azure Storage, Azure SQL, Private DNS Zones, NSG Rules, Azure Firewall

Frameworks: Zero Trust Architecture, ISO/IEC 27001:2022

Project Summary

Designed and implemented a secure Azure architecture by eliminating all public internet exposure for sensitive resources using private endpoints, DNS zone mapping, and layered network restrictions. Applied Azure Firewall, NSG rules, and private DNS zones to achieve a 100% reduction in public exposure, in alignment with Zero Trust principles and ISO/IEC 27001:2022 controls.

Objectives

• Restrict public network access to Azure Storage and Azure SQL using private endpoints only.

• Implement Azure Firewall to control all outbound and inbound traffic with explicit allow rules.

• Configure Private DNS Zones for secure resource resolution without public DNS queries.

• Enforce NSG rules to segment and protect subnets according to least-privilege principles.

• Align security configurations to ISO/IEC 27001:2022 control objectives.

Scope

• Applies to Azure resources hosting sensitive workloads (Azure Storage, Azure SQL).

• Removes all public IP addresses and disables public network access.

• Implements DNS zone mapping to ensure private-only resolution of endpoints.

• Uses Azure Firewall for centralized traffic inspection and filtering.

• NSG rules applied for subnet-level access control.

Implementation Steps

1. Provisioned Azure Storage and Azure SQL with public network access disabled.

2. Created Private Endpoints in dedicated subnets for both resources.

3. Configured Private DNS Zones and linked them to the virtual network for name resolution.

4. Deployed Azure Firewall with allow rules for necessary services and deny rules for all else.

5. Applied NSG rules to restrict subnet traffic according to Zero Trust principles.

6. Validated that resources were accessible only from within the virtual network.

ISO/IEC 27001:2022 Control Mapping

Control	Goal	Coverage
A.8.20 – Network Security	Ensure networks are protected against unauthorized access and attacks.	All sensitive resources isolated within private subnets; NSG and Firewall rules enforce access restrictions.
A.8.23 – Web Filtering	Restrict access to unauthorized or malicious web destinations.	Azure Firewall rules block all outbound internet traffic except approved destinations.
A.8.21 – Security of Network Services	Ensure network services are securely configured and managed.	Private DNS zones ensure internal name resolution; no public DNS queries permitted.

Results & Impact

• Public exposure reduced from 100% to 0% for targeted Azure resources.

• Enforced Zero Trust controls for network segmentation and access.

• Achieved compliance with ISO/IEC 27001:2022 network security objectives.

• Reduced attack surface significantly, mitigating risk of data exfiltration via public endpoints.

Key Skills Demonstrated

• Azure network security architecture and Zero Trust implementation.

• Private endpoint configuration and DNS zone management.

• Azure Firewall and NSG rule design for least privilege.

• Compliance mapping to ISO/IEC 27001:2022 controls.